



**STATE OF WASHINGTON
SECRETARY OF STATE**

ELECTRONIC AUTHENTICATION OPERATIVE PERSONNEL EXAM

INSTRUCTIONS

Please circle the correct answer in ink pen. Multiple answers will result in the question being marked as having been answered incorrectly. Select the best answer from the options given.

You must correctly answer at least 30 questions to pass.

The exam is open-book, and there is no time limit, but you may only take this exam one time within any thirty-day period. Any written materials may be referred to except for the operative personnel exam answer keys, whether the key has been prepared by this office or not. **You may not discuss this exam, the questions or your answers with any other person until you have submitted the test for grading.** Please return the test to:

OFFICE OF THE SECRETARY OF STATE
DIGITAL SIGNATURE PROGRAM
505 E. UNION
PO BOX 40234
OLYMPIA, WA 98504-0234

Be sure to include the examination grading fee of \$50.00. Checks should be made payable to "Secretary of State."

Enter your name, address and telephone number in the space provided below:

First _____ Middle _____ Last _____

Mailing Address _____

City _____ State or Country _____

Zip or Postal Code _____

Telephone Number _____

Test results will be mailed to the address listed above, and a copy of the exam results must be included in the Application for Certification as Digital Signature Operative Personnel.

ELECTRONIC AUTHENTICATION OPERATIVE PERSONNEL EXAM

1. Which of the following is not a stated purpose of the Washington Electronic Authentication Act?
 - A. Facilitate commerce by means of reliable electronic messages.
 - B. Promote access and communication between the public and government agencies.
 - C. Minimize the incidence of forged or fraudulent digital signatures.
 - D. Establish, in coordination with multiple states, uniform rules regarding the authentication and reliability of electronic messages.

2. Which of the following is not required by a certification authority to be licensed by the Washington Secretary of State?
 - A. The certification authority's principal place of business must be located in the State of Washington.
 - B. The certification authority must use a "trustworthy system" as defined under the Washington Electronic Authentication Act.
 - C. The certification authority must be the subscriber of a certificate published in a recognized repository.
 - D. The certification authority must employ individuals who have not been convicted of a crime involving fraud or dishonesty.

3. Which of the following statements is true?
 - A. A licensed certification authority may assign any individual to perform the functions of operative personnel, even if that individual has not been certified, for a reasonable period of time during the certification process so long as an application has been filed with the Washington Secretary of State.
 - B. A licensed certification authority may not assign any individual to perform the functions of operative personnel until it has notified the Washington Secretary of State of its intent to do so, and received the approval of the Washington Secretary of State, or at the time of licensing renewal.
 - C. A licensed certification authority may not assign any individual to perform the functions of operative personnel if that individual has not been certified by the Washington Secretary of State.
 - D. None of the above.

4. If a licensed certification authority fails to comply with the Washington Electronic Authentication Act, the Act gives the Washington Secretary of State the authority to:
 - A. Revoke or suspend a certification authority's license.
 - B. Publish information about the violation in any newspaper.
 - C. Revoke the certification authority's business license.
 - D. Bring an action against the certification authority for violation of the Consumer Protection Act.

5. If a certification authority fails to obtain a license from the Washington Secretary of State's office, the Washington Electronic Authentication Act provides that:
- A. The certification authority may not issue certificates in the State of Washington.
 - B. The certification authority may not conduct any business in the State of Washington.
 - C. The certification authority will be liable for any loss caused by reliance on a certificate issued by such certification authority.
 - D. The Washington Electronic Authentication Act does not apply to such certification authority, except as specifically provided.
6. The Washington Secretary of State may order the summary suspension of a certification authority license if the Washington Secretary of State includes within a written order a finding that the certification authority has:
- A. Utilized its license in the commission of a violation of a state or federal criminal statute or of chapter 19.86 RCW.
 - B. Engaged in conduct giving rise to a serious risk of loss to public or private parties if the license is not immediately suspended.
 - C. Either one of the above.
 - D. None of the above.
7. Which of the following is not required before a licensed certification authority may discontinue its services?
- A. The licensed certification authority must minimize to the extent commercially reasonable any disruption to the subscribers of valid certificates and relying parties.
 - B. The licensed certification authority must sell all of its business to another licensed certification authority.
 - C. The licensed certification authority must notify all subscribers listed on valid certificates listed by the certification authority.
 - D. The licensed certification authority must make reasonable arrangements for preservation of the certification authority's records
8. Which of the following is not required before a licensed certification authority may issue a certificate to a subscriber?
- A. The certification authority has received a signed request by a prospective subscriber.
 - B. The certification authority has confirmed that the subscriber is the person to be listed in the certificate.
 - C. The certificate provides information sufficient to locate the repositories in which notification of the revocation or suspension of the certificate would be listed.
 - D. The certification authority has issued a password for the subscriber's private key.
9. In which of the following circumstances is a licensed certification authority not required to immediately revoke a certificate?
- A. The certification authority has decided to discontinue its business.
 - B. The certification authority determines that the certificate was not issued as required by the Washington Electronic Authentication Act.
 - C. The certification authority receives a certified copy of the subscriber's death certificate.
 - D. The subscriber is a corporation that has been dissolved.

10. If the certification practice statement of a licensed certification authority provides that the certification authority does not verify that the private key held by the subscriber corresponds to the public key listed in the subscriber's certificate, that certificate is:
- A. Valid under the Washington Electronic Authentication Act.
 - B. Not valid under the Washington Electronic Authentication Act.
 - C. Valid under the Washington Electronic Authentication Act only if it includes the disclaimer.
 - D. None of the above.
11. After a subscriber accepts a certificate from a licensed certification authority, the licensed certification authority must:
- A. Give to the subscriber the public and private keys, and password necessary to create a digital signature.
 - B. Must send information regarding the certificate to the Washington Office of the Secretary of State.
 - C. Must publish the certificate in a licensed or unlicensed repository.
 - D. Must publish a signed copy of the certificate in a recognized repository.
12. If the Washington Secretary of State decides to publish in a repository a statement regarding a licensed or unlicensed certification authority advising subscribers and relying parties about potential risks created by such certification authority:
- A. The Secretary of State must first hold a hearing before publishing a statement.
 - B. The certification authority named in the statement may file a written defense of 1,000 words or less responding to the Washington Secretary of State.
 - C. The certification authority named in the statement may file a written defense of 10,000 bytes or less.
 - D. The certification authority named in the statement may not file a statement in defense.
13. Under the Washington Electronic Authentication Act, a licensed certification authority, when using a certificate, is not required to give which of the following warranties?
- A. The certificate is valid in all states which recognize digital signatures.
 - B. The certificate contains no information known to the certification authority to be false.
 - C. The certificate satisfies all material requirements of the Washington Electronic Authentication Act.
 - D. The certification authority does not exceed any limits of its license in issuing the certificate.
14. Under the Washington Electronic Authentication Act, a licensed certification authority, upon issuance of a certificate, agrees to do which of the following:
- A. Obtain cross-certification from other states authorizing the use of digital signatures.
 - B. Notify the subscriber of any changes in the Washington Electronic Authentication Act.
 - C. To act promptly to suspend or revoke a certificate in accordance with the Washington Electronic Authentication Act.
 - D. Monitor all signatures by the subscriber to make sure that the subscriber's private key has not been compromised.

15. Under the Washington Electronic Authentication Act, a licensed certification authority, upon issuing a certificate to a subscriber, is not required to certify which of the following to parties who rely on such certificate:
- A. The subscriber, at the time of use, has control of his or her private key.
 - B. The information in the certificate and listed as confirmed by the certification authority is accurate.
 - C. All information foreseeable material to the reliability of the certificate is stated or incorporated by reference within the certificate.
 - D. The subscriber has accepted the certificate.
16. If a potential subscriber (seeking a certificate from a licensed certification authority) states that it is an agent on behalf of another person or entity, the licensed certification authority may issue a certificate to such agent only if:
- A. The subscriber duly authorized the agent to have custody of the subscriber's private key.
 - B. The subscriber duly authorized the agent to request issuance of a certificate listing the corresponding public key.
 - C. Only if A and B are satisfied.
 - D. None of the above, because an agent may not obtain a certificate on behalf of a principal.
17. If a subscriber publishes information about the subscriber's private key on a publicly assessable Web page, the Electronic Authentication Act and relevant administrative rules state that the subscriber may be found to be:
- A. Liable for any losses incurred as a result of disclosure of information about the private key.
 - B. Only liable if a court of law determines that the subscriber intentionally published information about the private key.
 - C. Not liable from any loss relating to the disclosure of information about the private key in excess of \$50.
 - D. Not liable for any loss caused by disclosure of information about the private key.
18. Which of the following best describes the NIST CS-2 Protection Profile?
- A. A description of parameters available in defining a certificate profile.
 - B. A generalized certificate structure.
 - C. A baseline set of security functions and assurances.
 - D. A set of uniform rules regarding the authenticity and reliability of electronic messages.
19. Immediately upon suspension of a certificate by a licensed certification authority, the licensed certification authority must:
- A. Notify the Secretary of State.
 - B. Notify all relying parties.
 - C. Give notice of the suspension according to the specifications in the certificate.
 - D. All of the above.

20. If a licensed certification authority commits a violation of chapter 19.34 RCW, which of the following actions may the Secretary take:
- A. Order the licensed certification authority to stop doing business in the State of Washington.
 - B. Order that a civil penalty be imposed against the licensed certification authority.
 - C. Refuse to allow the licensed certification authority to apply for recognition of their repository.
 - D. None of the above.
21. If, upon suspension of a certificate by a licensed certification authority, the repository listed in the certificate no longer exists or refuses to accept publication of the suspension, the certification authority must:
- A. Give notice of the suspension to the Secretary of State.
 - B. Give notice to the Secretary of State that repository no longer exists or refuses to accept publication.
 - C. Publish a notice of the suspension of the certificate in any recognized repository.
 - D. None of the above.
22. Which of the following must be included in a certificate issued by a licensed certification authority?
- A. Information sufficient to locate or identify one or more repositories in which notification of the revocation or suspension of the certificate will be listed if the certificate is suspended or revoked.
 - B. The date on which the certificate expires.
 - C. Both A and B.
 - D. None of the above.
23. The NIST CS-2 Protection Profile makes a series of secure usage assumptions. These assumptions include:
- A. That at least some of the system components are physically protected.
 - B. That authorized users will be able to connect to the system remotely over an unprotected network.
 - C. Both of the above.
 - D. None of the above.
24. Which of the following is a true statement?
- A. The licensed certification authority must confirm a request for revocation and revoke a certificate within four (4) hours after receiving a subscriber's written request.
 - B. A licensed certification authority must confirm a request for revocation and revoke a certificate within four (4) hours after receiving both a subscriber's written request and evidence reasonably sufficient to confirm the identity and agency of the person requesting the revocation.
 - C. A licensed certification authority must confirm a request for revocation and revoke a certificate within one (1) business day after receiving a subscriber's written request for revocation.
 - D. A licensed certification authority must confirm a request for revocation and revoke a certificate within one (1) business day after receiving both a subscriber's written request and evidence reasonably sufficient to confirm the identity and any agency of the person requesting the revocation.

25. What is the recommended reliance limit in a certificate?
- A. The cumulative amount of transactions for which the subscriber may use the digital signature associated with the certificate.
 - B. The amount above which a transaction involving the digital signature is not valid.
 - C. The amount above which a licensed certification authority is not liable for a loss caused by reliance on a false or forged signature of the subscriber.
 - D. All of the above.
26. When a licensed certification authority conducts its operations within the terms of the Washington Electronic Authentication Act, that licensed certification authority is not liable for which of the following types of damages?
- A. Punitive damages.
 - B. Exemplary damages.
 - C. Damages for pain and suffering.
 - D. All of the above.
27. Which of the following is not a security objective of the NIST CS-2 standards?
- A. The system must ensure that all system users can subsequently be held accountable for actions which may impact upon the security of the system.
 - B. The system must provide a reasonable means for the acceptance of messages validated by a digital signature.
 - C. The system or its operators must provide a procedure for recovery in the event of a system failure or discontinuity of service.
 - D. The system must limit user access to only those system resources for which the user has been granted access.
28. What is the effect of a valid digital signature under the Washington Electronic Authentication Act?
- A. The digital signature is valid so long as the certificate corresponding to the digital signature has not expired.
 - B. The digital signature satisfies any rule of law requiring a signature.
 - C. The digital signature is only valid if the contract is governed by Washington law.
 - D. None of the above.
29. If a subscriber, in the process of applying for a certificate from a licensed certification authority, instructs the certification authority in writing that he or she wishes to waive the requirement that the certification authority confirm that the private key held by the subscriber is capable of creating a digital signature, the licensed certification authority:
- A. May issue a certificate to such subscriber under those conditions.
 - B. May not issue a certificate to such subscriber under those conditions.
 - C. May issue a certificate to such subscriber but only if the certificate includes information that the subscriber has waived the foregoing requirement.
 - D. None of the above.
30. A digital signature satisfies a rule of law requiring a signature if:
- A. The digital signature is verified by reference to the public key listed in a valid certificate issued by a licensed certification authority.
 - B. The digital signature was affixed by the signer with the intention of signing the message.
 - C. The recipient has no knowledge or notice that the signer either breached a duty a subscriber or does not rightfully hold the private key used to affix the digital signature.
 - D. All of the above are satisfied.

31. In which ways may recognition of a repository be discontinued?
- A. Upon thirty (30) days written notice to the Secretary of State by the recognized repository.
 - B. The Secretary of State discontinues recognition of a repository in accordance with the Administrative Procedures Act.
 - C. Either A or B.
 - D. None of the above.
32. Which of the following statements regarding the NIST CS-2 protection profile is false?
- A. Systems that meet the CS-2 protection standards are not necessarily designed to enforce controls on the flow of information between objects at differing levels of information sensitivity.
 - B. In commercial environments, CS-2 compliant systems are considered to be suitable to protect information such that only designated groups of users may access the information.
 - C. CS-2 compliant systems are considered to be suitable to protect sensitive-but-unclassified information in government environments.
 - D. None of the above.
33. When must a licensed certification authority revoke a certificate that it issued?
- A. After receiving a request for revocation by the subscriber named in the certificate.
 - B. After receiving a request for revocation by the subscriber of any transactional certificate.
 - C. After receiving a request for revocation by the subscriber named in the certificate and the licensed certification authority has confirmed that the person requesting revocation is the subscriber, or is an agent of the subscriber with authority to request revocation.
 - D. None of the above.
34. Which of the following types of records is a licensed certification authority required to preserve?
- A. Notices of suspension of certificates.
 - B. A database file containing records of the identity of every subscriber named in each certificate issued by the certification authority.
 - C. A database file of every time-stamp issued by the certification authority.
 - D. All of the above.
35. What is the purpose of the "Key Usage" extension as described in X.509?
- A. Allows the certificate issuer to specify a different validity period for the private key than the certificate.
 - B. Defines the purpose of the key contained in the certificate.
 - C. It contains a sequence of one or more policy information terms, each of which consists of an object identifier (OID) and optional qualifiers.
 - D. None of the above.
36. The published certification practice statement of a licensed certification authority is not required to contain which of the following?
- A. The price the certification authority is charging for each certificate in a given class.
 - B. Any warnings, liability limitations or warranty disclaimers upon which the certification authority intends to rely.
 - C. A disclosure of any mandatory dispute resolution process, if required by the certification authority.
 - D. The methods of subscriber identification applicable to any class of certificate issued.

37. A licensed certification authority's system is regarded as trustworthy where it:
- A. Has been audited by a certified public accountant who is generally familiar with information technology systems.
 - B. Materially satisfies the common criteria protection profile for commercial security 2, as published by the National Institute of Standards and Technology.
 - C. Both of the above.
 - D. None of the above.
38. What is one of the defined purposes of certificate extensions?
- A. Allow for the general use of digital signatures over unprotected networks.
 - B. Provide unique identifiers to prevent the reuse of subject names over time.
 - C. Provide methods for associating additional attributes with users or public keys.
 - D. None of the above.
39. The Authority Information Access extension in a certificate indicates:
- A. The class of persons who are authorized to view the information contained in a certificate.
 - B. How to access certification authority information and services for the issuer of the certificate in which the extension appears.
 - C. The object identifier which can be used to obtain a description of the certification authorities that have issued certificates superior in the public key infrastructure hierarchy to the certification authority that issued the certificate containing the extension.
 - D. None of the above.
40. In addition to the requirements of WAC 434-180-360, in order to be considered a trustworthy system a recognized repository must also:
- A. Possess the capacity to process transactions in a manner reasonably adequate for anticipated volume.
 - B. Provide for the periodic storage of back-up data at a location other than that which houses the principal system utilized for the repository.
 - C. Both of the above.
 - D. None of the above.

AFFIRMATION

I certify under penalty of perjury under the laws of the State of Washington that I have personally completed the foregoing examination, that I have not taken an examination for certification as operative personnel pursuant to Washington law within the past thirty days, and that the foregoing is true and correct.

Signature

Printed Name

Date & Place